

FILED

MAY 01 2012

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF

A TWO STORY RESIDENCE AND TWO DETACHED
~~OUTBUILDINGS~~ LOCATED AT
621 GREENWOOD PLACE
COLLINSVILLE, ILLINOIS 62234

5-1-12

Case No.

12-mj-3082-DGW

FILED UNDER SEAL

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

I, David J. Wargo, being duly sworn depose and say:

I am a Special Agent of the Illinois State Police, and have reason to believe that on the premises known as:

621 Greenwood Place, Collinsville, Illinois, which is more particularly described as a single residence with the numbers "621" above the front and back doors. This is a two story dwelling with white siding, wood stained front door and white trimmed storm door. The dwelling sits on the corner of Greenwood Place and Grandview Drive, facing Greenwood Place. The residence has a small wooden front porch with a white mailbox to the side of the porch. The mailbox has the numbers "621" on the front of it. The residence also has a wooden deck on the back of the residence. There were two "outbuildings" in the back, not attached to the residence. Each of those buildings are white, one had an overhead garage doors, and the other appeared to be a shed. (see attached photos).

and which residence is located in Madison County, within the Southern District of Illinois, there is now concealed certain property, including

SEE ATTACHED LIST ENTITLED "ATTACHMENT A"

which constitutes evidence of the commission of a criminal offense or which is contraband, the

fruits of crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of committing an offense; all in violation of Title 18, United States Code, Sections 2252 and 2252A, specifically evidence related to the possession and/or distribution of images of minor(s) engaged in sexually explicit activity and other sections of the United States criminal statutes. The facts to support the issuance of a search warrant are as follows:

AFFIDAVIT

1. I am a Special Agent of the Illinois State Police, and have been so employed for approximately 12 years. My current assignment is forensic examiner/investigator with the United States Secret Service – Southern Illinois Cyber-crime Unit. My training includes 192 hours training sponsored by the U.S. Secret Service in digital evidence and computer forensics examinations. I have over 300 hours of training recognized and certified by the Illinois Training and Standards Board and have been trained in the investigation of computer use in the exploitation of children as well as other digital investigations and evidence gathering. I am a member of the Illinois Attorney General's Internet Crimes Against Children Task Force. I have assisted Federal, State, and local agencies in digital investigations. I have, on several occasions, been involved with investigations involving internet/computer crimes and have been involved in the execution of numerous search warrants.

2. I make this affidavit in support of a warrant to search a residence located at 621 Greenwood Place, Collinsville, Illinois.

3. This affidavit seeks to search for and to seize contraband, evidence or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, specifically evidence related to the possession and/or distribution of images of minor(s) engaged

in sexually explicit activity.

4. The statements contained in this affidavit are based upon my training and experience as a Special Federal Officer of the United States Secret Service, information provided to me by other law enforcement officers and investigators, and upon my consultation with personnel trained in the investigation, seizure, and analysis of computers, electronic data, and electronic media. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a violation of Title 18, United States Code, Section 2252A exists at the residence known as 621 Greenwood Place, Collinsville, Illinois..

Computer Searches Generally

5. It is my belief that any number of the items sought in this affidavit for search warrant may be found, are items which stored electronically. Based upon my knowledge, training, and experience, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items. I know that electronic files can be easily moved from one computer or electronic storage medium to another. Therefore, electronic files downloaded to or created on one computer can be copied on or transferred to any other computer or storage medium at the same location. In addition, I know that searching computerized information for evidence of crimes often requires Special Agents to seize most or all of a computer system's

central processing unit (“CPU”) and/or laptop computer, input/output peripheral devices, related software, documentation, storage media, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. This is true because of the following:

a. Volume of evidence: Electronic media and storage devices such as hard disks, CD-ROMs, DVDs, diskettes, tapes and laser disks can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all of the stored data to determine which particular files is evidence or instrumentalities of crime. This sorting process can take weeks to months, depending on the volume of data stored. It would also be impractical to attempt this type of data search on site.

b. Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert and examiner is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system such as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

c. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different

techniques. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the pertinent files, in order to locate the evidence and instrumentalities authorized for seizure by the warrant); “opening” or reading the first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; or performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

d. Latent data: Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until its is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer’s operating system may also keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer’s settings in the event of a system failure.

e. Contextual data: In some instances, the computer “writes” to storage media without the specific knowledge or permission of the user. Generally, data or files that

have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

1. Digital data on the hard drive that is not currently associated with any file, may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

2. Further, evidence of how a digital device has been used, what it

has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that are no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage, and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Child Pornography Collector Characteristics

6. Based upon my knowledge, training, and experience, I am aware child pornography distributors/collectors:
 - a. Receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity.
 - b. Collect sexually explicit or suggestive materials (hard-core and soft-core pornography, whether of adults and/or of children) in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that

they use for their own sexual arousal and gratification.

c. Almost always possess and maintain their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, child erotica, etc.) in the privacy and security of their homes or some other secure location.

Child pornography distributors/collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years, and store their child pornography amongst other, otherwise legal, media or files.

d. Often correspond and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals whom they have been in contact and who share the same interests in child pornography.

e. Often maintain their collection of child pornography in computer files located on a computer's hard drive or other computer media and that these computer files or remnants of such files can be recovered months or even years after they have been downloaded on to a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache". The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Peer to Peer File Sharing

7. A growing phenomenon on the Internet is peer to peer file sharing (hereinafter, "P2P"). P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. Based upon my knowledge, training, and experience, I know the following is true of P2P file sharing:

a. There are several P2P networks currently operating (i.e. Gnutella, e-Mule and Ares) and several different software applications that can be used to access these networks (i.e. Limewire, Bearshare and Phex) but these applications operate in essentially the same manner.

b. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the network. This rating affects the user's ability to download files. The

more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is not required to share files to utilize the P2P network.

c. A user generally obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then selects file(s) which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Often times a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained. Furthermore, as mentioned above, even if a user chooses to delete files from his/her shared folder, the deleted files are generally able to be recovered.

d. A person interested in sharing child pornography with others in the P2P network, need only save those files in his/her "shared" folder(s). Those child pornography files are then available to all users of the P2P network for download regardless of their physical location.

e. A person interested in obtaining child pornography could open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select files from the search results and

those files can be downloaded directly from the computer(s) sharing those files.

f. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person that includes child pornography files in his/her "shared" folder is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography. A person that hosts child pornography is in violation of Title 18 Section 2252A(a)(3)(B) in that he/she is promoting and presenting child pornography in interstate and foreign commerce by means of a computer.

g. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can select and download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading a video file may actually receive parts of the file from multiple computers. The advantage of this is that it reduces the time it takes to download the file. A P2P file transfer is accomplished, like all Internet data transmission, by use of an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular Internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

h. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active

participation.

i. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded.

Background of Investigation

8. During an authorized undercover internet investigation, your affiant, utilizing software configured to search the Gnutella network (a public file sharing network) identified a computer with Internet Protocol (IP) address 75.132.216.137 that was offering to participate in the distribution of child pornography via a peer-to-peer (P2P) network. This identification took place on 03/28/12 at 4:33:21 a.m with a GMT offset of -5 hours.

9. On 03/28/12 at 4:33:21 a.m with a GMT offset of -5 hours, I obtained a list of known child pornography files (including file names and Sha1 values) which IP address 99.152.33.26 had available, at least in part, for download. The list contained 33 movie files, which had names indicative of the files containing child pornography. The list also captured the globally unique identification (GUID), which is the unique reference number used as an identifier in computer software installations. The version of P2P software was reported as LimeWire (Pro) version 4.12.11 and the GUID was reported as 603CE6C75816CD40BFA9A8A4B6250200.

On several occasions, I attempted to connect directly to the computer at IP address 75.132.216.137, but was unable to do so.

Your affiant knows that computer software has different methods to insure that two files are exactly the same. Your affiant knows from training and experience that the method used by the

Gnutella network involves a file encryption method called Secure Hash Algorithm Version 1 or SHA1. A SHA1 is the Secure Hash Algorithm (SHA), developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS).

Digital files can be processed by this SHA1 process resulting in a unique digital signature. By comparing these signatures it can be concluded that two files are identical with a precision that greatly exceeds 99.9 percent certainty.

Based on the SHA1 values of the files which IP address 75.132.216.137 had available, at least in part, on 03/28/12, I was able to connect to other users of the Gnutella network and download the following two files, which had the same SHA1 values as two files on the list IP address:

**(Yamad Boy)Zadoom Pedo Russian Boy 11Yr With Long Cock Andy's Friend1 2Of2
Bibcam - 2 Boys Having Fun (Andy And Friend).mpg**
SHA1: YD3OMPPEYQN6FMS33PWFCU3XUC2IFFXC

DESCRIPTION: VIDEO FILE (0 MINUTES 25 SECONDS) DEPICTING THE LASCIVIOUS DISPLAY OF TWO MALE CHILDREN MASTURBATING EACH OTHER. BOTH MALE CHILDREN APPEAR TO BE APPROXIMATELY 9-11 YEARS OLD. THE VIDEO ZOOMS IN ON THE NUDE PUBIC REGION OF EACH CHILD.

The above file completed download on 03/29/12 at approximately 10:05 a.m. from multiple sources.

Bibcam - Vegard - 12yo.avi
SHA1: 4BVWLOUD5ZFC2733N43QUY6TM66A35ZEP

DESCRIPTION: VIDEO FILE (2 MINUTES AND 52 SECONDS) DEPICTING THE LASCIVIOUS DISPLAY OF A MALE CHILD USING A WEBCAM TO VIDEOTAPE HIS ERECT PENIS. THE MALE CHILD IS APPROXIMATELY 11-12 YEARS OLD.

The above file completed download on 03/29/12 at approximately 6:28 p.m. from multiple sources.

On 04/03/12, I viewed the above files and based on my training and experience, believe the files

contain child pornography as defined in Federal Statute 18 U.S.C. 2252(a)(4)(B). I compared the SHA1 hash value of the files I downloaded from multiple users over the Gnutella network with the SHA1 value of the files which IP address 75.132.216.137 had available, at least in part, on 03/28/12 and those values matched.

10. A check with the American Registry of Internet Numbers (ARIN) showed the IP address 75.132.216.137 registered to Charter Communications. An administrative subpoena was issued from the United States Attorney's Office (Southern District of Illinois) in Fairview Heights, Illinois to Charter Communications to determine which subscriber was issued IP address 75.132.216.137 on 03/28/12 at 4:33:21 a.m. (CDST). The date and time indicates when the IP address 75.132.216.137 had child pornography files available for download, at least in part.

11. In response to the federal subpoena, subscriber information for IP address 75.132.216.137 on 03/28/12 at 4:33:21 a.m. (CDST) was provided on 04/13/12, by Charter Communications. The documents provided by Charter Communication showed the subscriber for IP address 75.132.216.137 as:

IP Address: 75.132.216.137
Start Time (GMT): 2011-11-07 @ 14:53:11
End Time (GMT): 2012-04-11 @ 17:37:25
Account Holder: Jonathan Mills
Service Address: 621 Greenwood Place
Collinsville, IL 62234
Account: 8345782020157442
Service Number: 6182238157
Type of Service: Internet, video and telephone
Payment Info: Visa (last 4 of card 1942, preceding digits not available to Charter)

I have been to Collinsville, Illinois and photographed the residence at 621 Greenwood Place. The building is a two story "cape cod" style home with white siding and gray shingle

roof. Both the front door and the back door have the numbers "621" directly above each door. There were two "outbuildings" in the back, not attached to the residence. Each were white, one had an overhead garage door, while the other appears to be a shed. There was a green Dodge Grand Caravan SE parked in the driveway with Illinois registration G889349. A registration check on the vehicle shows it is registered to Jonathan & Ruth Mills at 621 Greenwood PL, Collinsville, Illinois 62234-1441.

On 4/25/12, I drove by the residence at 621 Greenwood Place, Collinsville, Illinois. The green Dodge Grand Caravan was parked on the side of the residence, off Grandview Drive and there was a 2003 Mazda minivan parked in the driveway with Illinois registration 8227922. A registration check on the vehicle shows it is registered to Jonathan & Ruth Mills at 621 Greenwood PL, Collinsville, Illinois 62234-1441. I also conducted a search to determine when the last time IP address 75.132.216.137 was logged onto the Gnutella network, making available, at least in part, files which contain child pornography. The check showed IP address 75.132.216.137 was last identified on 04/14/12 at 2:34:41 am. On that date and time, IP address 75.132.216.137 had approximately 7 additional files (45 total videos) available for download, at least in part, with names indicative of the files containing child pornography.

Conclusion

12. Based on the foregoing information, I have probable cause to believe that evidence of violations of 18 U.S.C. § § 2252 and 2252A, as set forth herein and in Attachment A, are currently on the premises located 621 Greenwood Place, Collinsville, Illinois. I therefore respectfully request that a search warrant be issued authorizing the search for, seizure of, and search of, the items set forth in Attachment A.

13. Disclosure of the contents of the application and affidavit and the search warrant could compromise and jeopardize an ongoing investigation. For that reason, we request that the application and search warrant be sealed.

FURTHER AFFIANT SAYETH NAUGHT.



David J. Wargo
Special Federal Officer
United States Secret Service

STEPHEN R. WIGGINTON
United States Attorney


ALI SUMMERS
Assistant United States Attorney

State of Illinois)
) SS.
County of St. Clair)

Sworn to before me, and subscribed in my presence on the 1st day of May, 2012, at
East St. Louis, Illinois.


DONALD G. WILKERSON
United States Magistrate Judge

ATTACHMENT A

- (a) All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including, but not limited to, any computer, computer system and related peripherals including data processing devices; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, and other memory storage devices; peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.
- (b) Computer software, including, but not limited to, programs to run operating systems, applications, utilities, compilers, interpreters, video, web browsers, P2P programs, Fservices programs, and communications programs. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
- (c) Any and all documents, records, e-mails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography.
- (d) Electronic chat room and mail messages, notes, listings, and records relating to other individuals or entities involved in the production, distribution, or receipt of materials that depict or promote the sexual exploitation of children.
- (e) Visual depictions in whatever form created, stored, or printed which depict children under the age of 18 years engaged in sexually explicit conduct.
- (f) Any and all records, documents, invoices, notes and materials that pertain to ISP subscriber account billing statements, cable television bills, credit and debit card statements, bank statements, checks, money orders, telephone bills, and utility bills, and other documents which reflect the identity of the occupant(s) of the residence, as well as any and all records relating to the ownership or use of computer equipment found in the residence.
- (g) All of the foregoing items of evidence in whatever form and by whatever means such items may have been created or stored, including any handmade form, any photographic form, any mechanical form, or any electrical, electronic, or magnetic form, such as any information on an electronic or magnetic storage device like a floppy diskette, hard disk, backup tape, CD-Rom, video-tape, DVD, optical disc, electronic dialer, electronic notebook, as well as printout or readouts from any magnetic storage device.

